

SECTION 4. (a) The Tenth and Eleventh Administrative Judicial Regions are created on September 1, 2017.

(b) On September 1, 2017, the governor, with the advice and consent of the senate, shall appoint judges to serve as presiding judges in the Tenth and Eleventh Administrative Judicial Regions and any administrative judicial region in which a vacancy in office occurs because the presiding judge of a judicial region is no longer qualified to serve as the presiding judge of the region because of the composition of the region on that date.

(c) On September 1, 2017, the county in which a presiding judge appointed under Subsection (b) of this section resides shall provide adequate quarters for the operation of the applicable administrative judicial region.

(d) Not later than September 1, 2017, the regional presiding judges of the First through Ninth Administrative Judicial Regions:

(1) shall develop and adopt by majority vote budgets for the Tenth and Eleventh Administrative Judicial Regions that include an assessment for each county included in the area that will comprise the new regions; and

(2) may by majority vote transfer money, as necessary, from the existing judicial regions to the Tenth and Eleventh Administrative Judicial Regions.

(e) A judge or associate judge or coordinator assigned or appointed to a court in a county included in the First, Second, Third, Tenth, or Eleventh Administrative Judicial Region on September 1, 2017, continues to serve in that position until removed by the regional presiding judge.

SECTION 5. Except as otherwise provided by this Act, this Act takes effect immediately if it receives a vote of two-thirds of all the members elected to each house, as provided by Section 39, Article III, Texas Constitution. If this Act does not receive the vote necessary for immediate effect, this Act takes effect on the 91st day after the last day of the legislative session.

Passed the Senate on May 4, 2017: Yeas 30, Nays 1; the Senate concurred in House amendment on May 26, 2017: Yeas 30, Nays 1; passed the House, with amendment, on May 22, 2017: Yeas 145, Nays 1, one present not voting.

Approved June 15, 2017.

Effective June 15, 2017, except as otherwise provided by this Act.

**STATE AGENCY INFORMATION SECURITY PLANS,
INFORMATION TECHNOLOGY EMPLOYEES, AND ONLINE
AND MOBILE APPLICATIONS**

CHAPTER 955

S.B. No. 1910

AN ACT

relating to state agency information security plans, information technology employees, and online and mobile applications.

Be it enacted by the Legislature of the State of Texas:

SECTION 1. Subchapter C, Chapter 2054, Government Code, is amended by adding Sections 2054.0591 and 2054.0592 to read as follows:

Sec. 2054.0591. CYBERSECURITY REPORT. (a) Not later than November 15 of each even-numbered year, the department shall submit to the governor, the lieutenant governor, the speaker of the house of representatives, and the standing committee of each house of the legislature with primary jurisdiction over state government operations a report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in this state. The report must include:

- (1) *an assessment of the resources available to address the operational and financial impacts of a cybersecurity event;*
- (2) *a review of existing statutes regarding cybersecurity and information resources technologies;*
- (3) *recommendations for legislative action to increase the state's cybersecurity and protect against adverse impacts from a cybersecurity event;*
- (4) *an evaluation of the costs and benefits of cybersecurity insurance; and*
- (5) *an evaluation of tertiary disaster recovery options.*

(b) *The department or a recipient of a report under this section may redact or withhold information confidential under Chapter 552, including Section 552.139, or other state or federal law that is contained in the report in response to a request under Chapter 552 without the necessity of requesting a decision from the attorney general under Subchapter G, Chapter 552.*

Sec. 2054.0592. CYBERSECURITY EMERGENCY FUNDING. *If a cybersecurity event creates a need for emergency funding, the department may request that the governor or Legislative Budget Board make a proposal under Chapter 317 to provide funding to manage the operational and financial impacts from the cybersecurity event.*

SECTION 2. Subchapter F, Chapter 2054, Government Code, is amended by adding Section 2054.1184 to read as follows:

Sec. 2054.1184. ASSESSMENT OF MAJOR INFORMATION RESOURCES PROJECT. (a) *A state agency proposing to spend appropriated funds for a major information resources project must first conduct an execution capability assessment to:*

- (1) *determine the agency's capability for implementing the project;*
- (2) *reduce the agency's financial risk in implementing the project; and*
- (3) *increase the probability of the agency's successful implementation of the project.*

(b) *A state agency shall submit to the department, the quality assurance team established under Section 2054.158, and the Legislative Budget Board a detailed report that identifies the agency's organizational strengths and any weaknesses that will be addressed before the agency initially spends appropriated funds for a major information resources project.*

(c) *A state agency may contract with an independent third party to conduct the assessment under Subsection (a) and prepare the report described by Subsection (b).*

SECTION 3. Section 2054.133(c), Government Code, is amended to read as follows:

(c) *Not later than October 15 of each even-numbered year, each state agency shall submit a copy of the agency's information security plan to the department. Subject to available resources, the department may select a portion of the submitted security plans to be assessed by the department in accordance with department rules.*

SECTION 4. Subchapter F, Chapter 2054, Government Code, is amended by adding Section 2054.136 to read as follows:

Sec. 2054.136. DESIGNATED INFORMATION SECURITY OFFICER. *Each state agency shall designate an information security officer who:*

- (1) *reports to the agency's executive-level management;*
- (2) *has authority over information security for the entire agency;*
- (3) *possesses the training and experience required to perform the duties required by department rules; and*
- (4) *to the extent feasible, has information security duties as the officer's primary duties.*

SECTION 5. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Sections 2054.516 and 2054.517 to read as follows:

Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE

APPLICATIONS. (a) *Each state agency, other than an institution of higher education subject to Section 2054.517, implementing an Internet website or mobile application that processes any sensitive personally identifiable or confidential information must:*

(1) *submit a biennial data security plan to the department not later than October 15 of each even-numbered year, to establish planned beta testing for websites or applications; and*

(2) *subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.*

(b) *The department shall review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan to the state agency as soon as practicable after the department reviews the plan.*

Sec. 2054.517. DATA SECURITY PROCEDURES FOR ONLINE AND MOBILE APPLICATIONS OF INSTITUTIONS OF HIGHER EDUCATION. (a) *Each institution of higher education, as defined by Section 61.003, Education Code, shall adopt and implement a policy for Internet website and mobile application security procedures that complies with this section.*

(b) *Before deploying an Internet website or mobile application that processes confidential information for an institution of higher education, the developer of the website or application for the institution must submit to the institution's information security officer the information required under policies adopted by the institution to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. At a minimum, the institution's policies must require the developer to submit information describing:*

(1) *the architecture of the website or application;*

(2) *the authentication mechanism for the website or application; and*

(3) *the administrator-level access to data included in the website or application.*

(c) *Before deploying an Internet website or mobile application described by Subsection (b), an institution of higher education must subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party.*

(d) *Each institution of higher education shall submit to the department the policies adopted as required by Subsection (b). The department shall review the policies and make recommendations for appropriate changes.*

SECTION 6. As soon as practicable after the effective date of this Act, the Department of Information Resources shall adopt the rules necessary to implement Section 2054.133(c), Government Code, as amended by this Act.

SECTION 7. This Act takes effect September 1, 2017.

Passed the Senate on May 4, 2017: Yeas 31, Nays 0; the Senate concurred in House amendments on May 26, 2017: Yeas 31, Nays 0; passed the House, with amendments, on May 22, 2017: Yeas 144, Nays 0, one present not voting.

Approved June 15, 2017.

Effective September 1, 2017.

ELIGIBILITY REQUIREMENTS FOR REGISTRATION AS AN INTERIOR DESIGNER

CHAPTER 956

S.B. No. 1932

AN ACT

relating to eligibility requirements for registration as an interior designer.